



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

25.1.2

MAY 20, 2024

EFFECTIVE DATE

(05-20-2024)

PURPOSE

- (1) This transmits revised IRM 25.1.2, Fraud Handbook, Recognizing and Developing Fraud.

MATERIAL CHANGES

- (1) IRM 25.1.2.11 and its subsections were added to discuss fraud related to cases involving digital assets.
- (2) Editorial changes were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

This supersedes IRM 25.1.2 dated November 3rd, 2023.

AUDIENCE

Criminal Investigation (CI), Large Business & International (LB&I), Small Business/Self-Employed (SB/SE), Tax Exempt/Government Entities (TE/GE), and Taxpayer Services (TS).

Deborah Ngo, Acting Director
Office of Fraud Enforcement, SB/SE

25.1.2

Recognizing and Developing Fraud

Table of Contents

25.1.2.1 Program Scope and Objectives

25.1.2.1.1 Background

25.1.2.1.2 Authority

25.1.2.1.3 Roles and Responsibilities

25.1.2.1.4 Program Management and Review

25.1.2.1.5 Program Controls

25.1.2.1.6 Acronyms

25.1.2.1.7 Terms

25.1.2.1.8 Related Resources

25.1.2.2 Fraud Development Procedures

25.1.2.3 Indicators of Fraud

25.1.2.4 Investigative Techniques

25.1.2.5 Aiding and Abetting

25.1.2.6 Bankruptcy Fraud

25.1.2.7 Employment Tax Fraud

25.1.2.8 Excise Tax Fraud

25.1.2.8.1 Excise Tax Fraud—Fuel Taxes

25.1.2.8.2 Excise Tax Fraud—Wagering Tax

25.1.2.8.3 Excise Tax Fraud—Retailer Schemes

25.1.2.8.4 Excise Tax Fraud—Heavy Highway Vehicle Use Tax

25.1.2.8.5 Excise Taxes—Willful Failure to Pay

25.1.2.8.6 Section 4103 cases—Referrals to Collection Function

25.1.2.9 Return Preparer Fraud

25.1.2.10 FinCEN Query (FCQ)

25.1.2.10.1 Requesting Access

25.1.2.10.2 Search Procedures and Reporting Requirements

25.1.2.10.3 Annual Audit Procedures

25.1.2.10.4 Program Analyst Procedures

25.1.2.10.5 Maintenance and Removal of Access

25.1.2.11 Digital Asset Fraud

25.1.2.11.1 Indicators of Fraud in Digital Asset Cases

25.1.2.11.2 IRS Has Repeatedly Informed Taxpayers of the Requirement to Report Digital Asset Transactions

25.1.2.11.3 Use of FinCEN in Digital Asset Cases

25.1.2.1
(04-23-2021)
Program Scope and Objectives

- (1) The mission of the Office of Fraud Enforcement (OFE) is to promote compliance by strengthening the IRS response to fraud and by mitigating emerging threats. This includes:
 - Improving fraud detection and development to address areas of high fraud/risk noncompliance,
 - Cultivating internal and external partnerships to identify new treatment streams to enhance enforcement, and
 - Pursuing civil fraud penalties and recommending criminal cases that will lead to prosecutions, where appropriate.
- (2) **Purpose:** The primary purpose of this handbook is to assist civil compliance employees in recognizing indicators of fraud and to set forth the development process used to prove fraud.
- (3) **Audience:** This handbook is a comprehensive guide for IRS civil employees Servicewide in the recognition and development of potential fraud issues, referrals for criminal fraud, duties and responsibilities in joint investigations, civil fraud cases, and other related fraud issues.
- (4) **Policy Owner:** Director, Office of Fraud Enforcement, Small Business Self Employed (SB/SE).
- (5) **Program Owner:** Office of Fraud Enforcement Policy, SB/SE.
- (6) **Primary Stakeholders:** Employees in IRS compliance and the OFE.

25.1.2.1.1
(04-23-2021)
Background

- (1) This section discusses recognizing signs of fraud, known as first indicators (or badges) of fraud, and the development process used to prove fraud. Fraud is substantiated by establishing affirmative acts (firm indications) of fraud. Affirmative acts of fraud are actions taken by the taxpayer, return preparer and/or promoter to deceive or defraud.

25.1.2.1.2
(04-23-2021)
Authority

- (1) By law, the IRS has the authority to conduct examinations under Title 26, Internal Revenue Code Subtitle F – Procedure and Administration, Chapter 78, Discovery of Liability and Enforcement of Title, Subchapter A, Examination and Inspection.

25.1.2.1.3
(04-23-2021)
Roles and Responsibilities

- (1) The Director, Office of Fraud Enforcement, is the executive responsible for providing fraud policy and guidance for civil compliance employees and ensuring consistent application of policies and procedures in this IRM.
- (2) The Fraud Enforcement Advisor (FEA) serves as a resource and liaison to compliance employees in all operating divisions. The FEA is available to assist in fraud investigations and offer advice on matters concerning tax fraud.
- (3) Employees who work potential fraud cases are responsible for following the procedures in this IRM. All compliance employees and their managers working potential fraud cases should familiarize themselves with the information contained in this IRM.

25.1.2.1.4
(04-23-2021)

**Program Management
and Review**

- (1) The Office of Fraud Enforcement, Policy, prepares and issues the following reports to Servicewide customers:
 - Three-year reports prepared using Fraud Information Tracking System (FITS) data, and
 - Status 17 reports using Audit Information Management System (AIMS) or AIMS Centralized Information System (ACIS) data.
- (2) OFE Policy staff can create reports by area, territory or group. These reports help manage fraud inventory and provide review information for managerial use:
 - Cases on FITS but not on AIMS or ACIS,
 - Cases on AIMS or ACIS but not on FITS,
 - Cases in fraud development status, and
 - Cases in criminal fraud status.
- (3) Ad-hoc reports are produced as requested by OFE customers.
- (4) Operational reviews of the FEA group managers are completed by the OFE program manager twice a year. These reviews measure program consistency, effectiveness in case actions, and compliance with fraud policy and procedures.
- (5) FEA managers utilize reports generated from FITS to monitor and track FEA inventory assignments.

25.1.2.1.5
(04-23-2021)

Program Controls

- (1) FEA managers verify program and procedural compliance by conducting case consultations, case reviews, performance reviews, and security reviews with all FEAs.
- (2) FEAs are required to follow-up on all cases in fraud development status at least every 60 days as required by IRM 25.1.2.2, Fraud Development Procedures.
- (3) FEAs are required to monitor accepted criminal referrals each quarter to ensure that CI and compliance employees are holding productive quarterly meetings as required under IRM 25.1.4.4.4, Required Communications.

25.1.2.1.6
(04-23-2021)

Acronyms

- (1) See IRM 25.1.1.1.6, Acronyms and Codes.

25.1.2.1.7
(04-23-2021)

Terms

- (1) See IRM 25.1.1.1.7, Terms.

25.1.2.1.8
(04-23-2021)

Related Resources

- (1) See IRM 25.1.1.1.8, Related Resources.
- (2) See IRM 25.1.1.4, Indicators of Fraud vs. Affirmative Acts of Fraud, for further information regarding the difference between indicators of fraud and affirmative acts (firm indicators) of fraud.

25.1.2.2
(04-23-2021)
**Fraud Development
Procedures**

- (1) When indicators (badges) of fraud are uncovered, the compliance employee must clearly document the potential fraud indicators and initiate a discussion with the compliance employee's group manager. If the compliance employee's group manager concurs there are indicators of fraud warranting fraud development, the compliance employee must contact the fraud enforcement advisor (FEA). Initial contact with the FEA should be completed by submitting a request through the *Specialist Referral System (SRS)*. Campus employees do not use the SRS.

Note: For procedures specific to Campus Examination, see IRM 25.1.14, Campus Examination Fraud Procedures. Campus Collection procedures are located in IRM 25.1.11.7, Discussion with the Collection Functional Fraud Coordinator.

- (2) After reviewing the potential fraud indicators and possible barriers to a successful referral, if the compliance employee, compliance employee's group manager and FEA agree the potential for fraud exists, the compliance employee must prepare Form 11661, Fraud Development Recommendation – Examination, or Form 11661-A, Fraud Development Recommendation – Collection, and forward the completed form to the compliance employee's group manager for approval.

Note: Transmitting the forms electronically requires use of Microsoft Outlook Secure Messaging because of the confidential nature of the material (taxpayer information) it contains.

- (3) Form 11661/11661-A documents the FEA's involvement and places a case in fraud development status. A case must not be placed in or out of fraud development status without consulting the FEA. If disagreement exists on whether a case should be in fraud development status, the final decision rests with the compliance employee's group manager.
- (4) The compliance employee's group manager must review Form 11661/11661-A and indicate approval by entering their name and date, and electronically forward the completed form by secure messaging to the FEA for consideration.
- (5) When the FEA concurs with the fraud development determination, the FEA completes Form 11661/11661-A and returns it to the compliance employee and compliance employee's group manager, using secure messaging. A copy of the form must be placed in the Collection case file or in the Examination work papers; and a copy retained by the FEA. If a case is placed in fraud development status, a plan of action (plan) must be formulated as early as possible to develop and document the affirmative acts of fraud.
- (6) The initial plan and those containing follow up action items must be documented in the Collection Integrated Collection System (ICS) history or included in the Examination work papers; and a copy retained by the FEA. All contacts with the FEA and subsequent action plans must be accurately documented in the Collection case file or Examination work papers. The plan must:
 - a. Outline the steps required to establish affirmative acts (firm indications) of fraud,
 - b. Be the joint effort of the compliance employee, the compliance employee's group manager and the FEA,
 - c. Guide the case to its appropriate conclusion in a timely manner,

- d. Specify any direct assistance by the FEA. The role of the FEA can be advisory or consultive in nature, and
- e. There must be a follow up date documented on Form 11661/11661-A within 60 days of the initial Plan of Action and within 60 days of all subsequent action plans.

Note: Consultation with the FEA may or may not be face-to-face. Consultations over the phone, by e-mail, or virtual online meeting and sharing desktop information are possible; however, in-person contact is preferable.

- (7) The compliance employee, with the compliance employee's group manager's and FEA's concurrence, will place the case in fraud development status.
 - The revenue officer must request the input of ICS Sub-code 910 and/or upload of TC 971 AC 281 through the employee's group manager, as appropriate. See IRM 25.1.8.9, Aging of Collection Fraud Cases, for additional information.
 - The examiner must update the Audit Information Management System (AIMS) to status code 17. Cycle time is excluded from the monthly aging reports to management (Month At a Glance Report) for cases in fraud development status.
- (8) The compliance employee must request the original tax returns, if not already secured. For campus examination procedures on securing original returns, see IRM 4.19.10.4, Fraud Referrals. The compliance employee proceeds with the plan until affirmative acts of fraud are established or a determination is made that the potential for fraud no longer exists. Timely action is required on all cases in fraud development status.
- (9) If affirmative acts of fraud are established:
 - a. The compliance employee must suspend collection or examination activity, and immediately notify the group manager and the FEA.
 - b. The FEA recommends a referral to Criminal Investigation (CI), if criminal criteria is met (see IRM 25.1.3, Criminal Referrals).
 - c. If criminal criteria has **not** been met or the case is returned by CI subsequent to a criminal investigation, consideration of the civil fraud penalty under IRC 6663 and/or the fraudulent failure to file penalty under IRC 6651(f), and/or imposition of a 10-year ban under IRC 32(k)(1)(B)(i), IRC 24(g)(1)(B)(i), or IRC 25A(b)(4)(A)(ii)(I) is the shared responsibility of the compliance employee, the compliance employee's group manager and the FEA. The final decision rests with the compliance employee's group manager (see IRM 25.1.6.3, Procedures).
- (10) If the case is returned because the criminal criteria has not been met, or the case is returned by CI subsequent to a criminal investigation, determine if the taxpayer's actions were due to fraud and the criteria for a 10-year ban have been met. IRC 32(k) allows the IRS to impose bans on future claims of Earned Income Tax Credit (EITC) against taxpayers who made prior fraudulent claims for the EITC. The EITC 10-year ban is permitted after a **final determination** is made that the taxpayer's EITC claim was due to fraud. IRC 24(g)(1)(B)(i) allows the IRS to impose 10-year bans on future claims of Additional Child Tax Credit (ACTC)/Other Dependent Credit (ODC), against taxpayers where it is determined the taxpayer's actions were due to fraud. IRC 25A(b)(4)(A)(ii)(I) allows the IRS to impose 10-year bans on future claims of the American Op-

portunity Tax Credit (AOTC), against taxpayers where it is determined the taxpayer's actions were due to fraud. For jointly filed returns, consideration should be given to proposing a 10-year ban separately against each spouse. There should be a separate fraud write-up for each spouse, citing clear and convincing evidence of fraud on the part of each spouse. If the acts of only one spouse are found to be fraudulent, the 10-year ban will apply only to the culpable spouse. See IRM 20.1.5.3.5, Two and Ten Year Bans on Claiming the Earned Income Tax Credit (EITC), Child Tax Credit (CTC), Additional Child Tax Credit (ACTC), and American Opportunity Tax Credit (AOTC) and IRM 4.19.14.7.1, 2/10 Year Ban - Correspondence Guidelines for Examination Technicians (CET), for additional information.

- (11) A determination that the potential for fraud no longer exists:
- Is made by agreement of the compliance employee, the compliance employee's group manager, and the FEA. If an agreement cannot be reached, the compliance employee's group manager makes the final decision; and
 - Requires reversal of the Collection Sub-code 910 and/or TC 971 AC 281 (see IRM 25.1.8.9, Aging of Collection Fraud Cases); or return of the Examination case on AIMS to status 12 or other prior status code.

Caution: The compliance employee or the compliance employee's group manager must **never** seek advice from CI for a specific case under examination/ collection activity.

- (12) For a case that deviates from the established plan of action, the compliance employee's group manager or FEA should recommend return of the case to Collection field investigative status or to Examination status 12. See IRM 4.19.10.4, Fraud Referrals, for Campus examination procedures for returning the case to a prior status. A case is in fraud development status only while there is active FEA involvement in an ongoing audit or collection activity, or until the FEA recommends one of the following actions:
- Returning the Examination case to AIMS status 12, when it is determined that the potential for fraud no longer exists as evidenced by the reasons and decisions documented on Form 11661.
 - Removing the Collection Sub-code 910, via Form 11661-A, when it is determined that the potential for fraud no longer exists.
 - Asserting the civil fraud penalty under IRC 6663 and/or the fraudulent failure to file penalty under IRC 6651(f), and/or imposition of a 10-year ban under IRC 32(k)IRC 24(g)(1), or IRC 25A(b)(4)(A)(ii)(I) via Form 11661.

Note: The FEA also uses Form 11661 to recommend returning a case to Status 17 from Status 18. The ultimate decision with respect to all case action rests with the compliance employee's group manager.

25.1.2.3
(11-03-2023)

Indicators of Fraud

- (1) Listed below are categories of fraud indicators. Each category list is not intended to be all-inclusive, instead citing examples of actions taxpayers may take to deceive or defraud.
- (2) The following table shows indicators of fraud based on the taxpayer's income:

Indicators of Fraud—Income
Omitting specific items where similar items are included.
Omitting entire sources of income.
Failing to report or explain substantial amounts of income identified as received.
Inability to explain substantial increases in net worth, especially over a period of years.
Substantial personal expenditures exceeding reported resources.
Inability to explain sources of bank deposits substantially exceeding reported income.
Concealing domestic or foreign bank accounts, brokerage accounts, digital assets such as convertible virtual currency and cryptocurrency, or other property.
Inadequately explaining dealings in large sums of currency, or the unexplained expenditure of currency.
Consistent concealment of unexplained currency, especially in a business not routinely requiring large cash transactions.
Failing to deposit receipts in a business account, contrary to established practices.
Failing to file a tax return, especially for a period of several years, despite evidence of receipt of substantial amounts of taxable income.
Cashing checks, representing income, at check cashing services and at banks where the taxpayer does not maintain an account.
Concealing sources of receipts by false description of the source(s) of disclosed income, and/or nontaxable receipts.

- (3) The following table shows indicators of fraud based on the taxpayer's expenses and deductions:

Indicators of Fraud—Expenses or Deductions
Claiming fictitious or substantially overstated deductions.
Claiming substantial business expense deductions for personal expenditures.

Indicators of Fraud—Expenses or Deductions
Claiming dependency exemptions for nonexistent, deceased, or self-supporting persons. Providing false or altered documents, such as birth certificates, lease documents, school/medical records, for the purpose of claiming the education credit, additional child tax credit, earned income tax credit (EITC), or other refundable credits.
Disguising trust fund loans as expenses or deductions.

- (4) The following table shows indicators of fraud based on the taxpayer's books and record keeping:

Indicators of Fraud—Books and Records
Multiple sets of books or no records.
Failure to keep adequate records, concealment of records, or refusal to make records available.
False entries, or alterations made on the books and records; back-dated or post-dated documents; false invoices, false applications, false statements, or other false documents or applications.
Invoices are irregularly numbered, unnumbered or altered.
Checks made payable to third parties that are endorsed back to the taxpayer. Checks made payable to vendors and other business payees that are cashed by the taxpayer.
Variances between treatment of questionable items as reflected on the tax return, and representations within the books.
Intentional under- or over-footing of columns in journal or ledger.
Amounts on tax return not in agreement with amounts in books.
Amounts posted to ledger accounts not in agreement with source books or records.
Journalizing questionable items out of correct account.
Recording income items in suspense or asset accounts.
False receipts to donors by exempt organizations.

- (5) The following table shows indicators of fraud based on how the taxpayer allocates income:

Indicators of Fraud—Allocations of Income
Distribution of profits to fictitious partners.
Inclusion of income or deductions in the tax return of a related taxpayer, when tax rate differences are a factor.

- (6) The following table shows indicators of fraud based on the conduct and actions of the taxpayer:

Indicators of Fraud—Conduct of Taxpayer
False statement about a material fact pertaining to the examination.
Attempt to hinder or obstruct the examination. For example, failure to answer questions; repeated cancelled or rescheduled appointments; refusal to provide records; threatening potential witnesses, including the examiner; or assaulting the examiner.
Failure to follow the advice of accountant, attorney or return preparer.
Failure to make full disclosure of relevant facts to the accountant, attorney or return preparer.
The taxpayer's knowledge of taxes and business practices where numerous questionable items appear on the tax returns.
Testimony of employees concerning irregular business practices by the taxpayer.
Destruction of books and records, especially if just after examination was started.
Transfer of assets for purposes of concealment, or diversion of funds and/or assets by officials or trustees.
Pattern of consistent failure over several years to report income fully.
Proof that the tax return was incorrect to such an extent and in respect to items of such magnitude and character as to compel the conclusion that the falsity was known and deliberate.
Payment of improper expenses by or for officials or trustees.
Willful and intentional failure to execute pension plan amendments.
Backdated applications and related documents.
False statements on Tax Exempt/Government Entity (TE/GE) determination letter applications.
Use of false social security numbers.
Submission of false Form W-4.
Submission of a false affidavit.
Attempt to bribe the examiner.
Submission of tax returns with false claims of withholding (Form 1099-OID, Form W-2) or refundable credits (Form 4136, Form 2439) resulting in a substantial refund.
Intentional submission of a bad check resulting in erroneous refunds and releases of liens.
Submission of false Form W-7 information to secure Individual Taxpayer Identification Number (ITIN) for self and dependents.

- (7) The following table shows indicators of fraud based on how a taxpayer may hold title in, or use assets:

Indicators of Fraud—Methods of Concealment
Inadequacy of consideration.
Insolvency of transferor.
Asset ownership placed in other names.
Transfer of all or nearly all of debtor's property.
Close relationship between parties to the transfer.
Transfer made in anticipation of a tax assessment or while the investigation of a deficiency is pending.
A concealed interest in the property transferred.
Transaction not in the usual course of business.
Retention of possession or continued use of asset.
Transactions surrounded by secrecy.
False entries in books of transferor or transferee.
Unusual disposition of the consideration received for the property.
Use of secret bank accounts for income.
Deposits into bank accounts under nominee names.
Conduct of business transactions in false names.

25.1.2.4

(04-23-2021)

Investigative Techniques

- (1) The minimum plan of action must include following up on all leads identified as fraud indicators (signs or symptoms); securing copies of all relevant data relating to indicators of fraud; and noting from whom and when obtained.

Note: Original documents obtained from the taxpayer or third parties should not be marked, indexed, hole punched, or in any way altered by the compliance employee. Also, it is critical that the compliance employee attempt to secure the taxpayer's explanation(s) for any discrepancies.

- (2) In cases where a return has not been filed and fraud is suspected, the compliance employee must not demand a return from the taxpayer. A Letter 3798, Non-filer Appointment Letter, should be used in place of the regular initial appointment letter. Books and records pertaining to the unfiled year(s) should still be requested.
- (3) A Revenue Agent Report (Form 4549 or similar) must not be sent to the taxpayer and/or power of attorney unless and until this action is specifically discussed with the FEA.
- (4) Most fraud cases involve individual and business taxpayers with poor or non-existent internal controls and/or where there is little or no separation of duties. When these occur, there is a greater potential for material misstatement of taxable income than in cases involving individuals earning salaries and wages. However, fraud may be present in any type of tax return.

- (5) Unusual, inconsistent or incongruous items should alert compliance employees to the possibility of fraud and the need for further investigation. Taxpayer misconduct is an early warning sign of possible fraudulent conduct. The method of operating a business (i.e., lack of internal controls, dealing in cash, etc.) may be indicative of improperly filed tax returns. Consider all facts when determining the fraud risk factor. For example, when examining a cash-only business, consider the size and industry type.
- (6) The initial contact provides the opportunity to obtain valuable information, which may not be readily available later. Indications of fraud may be disclosed in discussions, financial activities and nonresponsive answers. Questions asked should be recorded verbatim. Similarly, nonresponsive answers should be noted verbatim and judgment used in deciding what information is relevant (affidavits may be used). Examination work papers should be noted as to the tax year, the date of the contact, who was present during the contact, and the author of the examination work papers.
- (7) Examination work papers must include the following information:
 - Who prepared the information used to complete the tax return,
 - Who approved and classified expense items,
 - Who deposited business receipts, and
 - How business gross receipts, per the tax return, were determined.
- (8) The compliance employee must prepare a Memorandum of Interview, summarizing information obtained and statements made. This becomes part of the Collection case file or Examination work papers, and aids in the fraud development.
- (9) Throughout the investigation, it is important to keep a current and accurate historical record of all contacts and conversations with the taxpayer. This is necessary to track statements when records were received and from whom; and steps taken to determine the accuracy of the information volunteered. Annotations must not be made on records and other evidence received. See IRM 25.1.2.4 (1), Investigative Techniques, for additional guidance. It is important that the chain of custody for evidence obtained is clearly established through the historical record. Although necessary in any investigation, this action can be critical in sustaining fraud.
- (10) Fraud is not ordinarily discovered when compliance employees readily accept the completeness and accuracy of records presented and explanations offered by the taxpayer. It is necessary to go behind the books and to probe beneath the surface to validate and determine the consistency of information provided and statements made to evaluate the credibility of evidence and testimony provided by the taxpayer. The judgment of the employee will determine the techniques used. The investigation is extended to the point where the employee is satisfied and the conclusions are substantially correct.

Note: The compliance employee must also consider identity theft issues during the course of an investigation. See IRM 25.23, Identity Protection and Victim Assistance, for additional guidance.

25.1.2.5
(06-09-2015)
Aiding and Abetting

- (1) It is important to determine who is responsible for the fraudulent act(s). If it is determined that the taxpayer is not the responsible party, then consideration should be given to determine if other related parties such as the preparer can be held responsible. If the preparer is culpable, then the Return Preparer Coordinator in your Area Planning and Special Programs (PSP) must be contacted. See IRM 20.1.6.3, Overview - Preparer and Promoter Penalties, IRC 6694 Understatement of Taxpayer's Liability by Tax Return Preparer and IRM 25.1.2.9, Return Preparer Fraud, for additional guidance.
- (2) Civil penalties apply to anyone who aids and abets an understatement of tax liability under IRC 6701. An individual who willfully aids and assists with the understatement of a tax liability can be criminally charged under Title 26 USC 7206(2). The individual must be directly involved in the preparation or presentation of the false or fraudulent document. This may include independent parties such as lawyers, accountants, return preparers, and appraisers who counsel on a course of action. It is possible for criminal referrals and/or civil penalties to apply to both the taxpayer and the person assisting the taxpayer. See IRM 4.32.2.2, Overview of Abusive Transactions (AT) Program.

25.1.2.6
(11-03-2023)
Bankruptcy Fraud

- (1) This section provides insight into the bankruptcy process and the ways a taxpayer may use bankruptcy to further an overt act in evading payment. For an in-depth discussion of bankruptcy fraud, compliance employees should refer to Document 9762, Desk Guide for Bankruptcy Tax Crime Referrals.
- (2) Bankruptcy is a federally authorized procedure by which a debtor (an individual, corporation, LLC, partnership or municipality) may be relieved of liability for certain debts pursuant to the statutory scheme contained in the Bankruptcy Code, 11 USC. In bankruptcy, creditors may be paid through the liquidation of the debtor's assets or through a court-approved repayment plan, depending on the type of bankruptcy filed. Individual debtors are allowed to claim some assets as "exempt", and those assets are not liquidated. Bankruptcy is intended to provide the debtor with a fresh start.
- (3) Preferably, bankruptcy fraud will be charged in conjunction with violations of the tax, money laundering, or currency statutes with CI's statutory jurisdiction. In instances where prosecution of these offenses is not practicable, prosecution can be recommended for bankruptcy fraud alone.
- (4) A bankruptcy case begins with the filing of a "petition" in the U.S. Bankruptcy Court. Creditors may also commence a bankruptcy case, however this is rare. Once the petition is filed, the bankruptcy "estate" is automatically created, which includes all of the debtor's property and interests in property, regardless of where the property is located and who is holding it. This includes real and personal property of all types, including cash. Further, if the debtor made a fraudulent transfer of any property within two years of filing the petition, that property may be brought into the bankruptcy **estate**. The bankruptcy code, *U.S. Code, Title 11*, provides a list of specific types of property that are excluded from the **estate**. In addition, debtors may exempt certain property from the **estate** by electing to apply statutory exemptions found in either state law or in the bankruptcy Code. In many cases a trustee is appointed as a representative of the **estate**. In cases filed under Chapter 7 of the bankruptcy code, a trustee is appointed to gather and liquidate those assets of the debtor that are not exempt. In a Chapter 11 case, the debtor generally remains in control of the assets and can continue to operate the debtor's business, if there is one. No trustee is appointed in these cases, and the debtor is responsible for

paying current operating expenses and making payments to creditors pursuant to a court-approved plan; however, see *11 U.S.C. 1104, Appointment of Trustee or Examiner*, which provides for appointing a Chapter 11 trustee in certain circumstances. In cases filed under Chapter 13 of the Bankruptcy Code, a trustee is appointed, but the debtor retains control of their assets, and the trustee's role is to collect payments from the debtor and to distribute the funds to the creditors pursuant to a court-approved plan. The trustee, if there is one, and any creditor may object to the allowance of the exemptions claimed. A trustee may also recover property, which was fraudulently transferred in the two-year period prior to the filing of the bankruptcy, or property that was a preferential transfer made to a creditor up to one year prior to the bankruptcy, depending on the creditor. A preferential transfer is one that gives the creditor a better recovery than the creditor would receive in the bankruptcy. If it is discovered that a debtor made fraudulent or preferential transfers and there is no trustee in the case, the transfers will serve as the basis for a creditor to request that a trustee be appointed to take control of the debtor's assets. See IRM 5.9.2.4, Chapters in Bankruptcy, for additional information.

- (5) A fraudulent conveyance is any transaction made with the intention of hindering the payment of tax due or to defraud the government through some other act, such as concealment or transfer of assets for less than the fair market value at a time when tax was due or would have become due if the return were filed. Most indications of bankruptcy fraud mirror those encountered by compliance employees in the course of routine investigations. Oftentimes, these cases involve entities that fail to keep ordinary records or follow generally accepted business practices.
- (6) A debtor must fully disclose its financial condition, including all assets, through a Statement of Financial Affairs (SOFA) filed at the beginning of the bankruptcy case. The SOFA contains numerous schedules that detail financial facts, income facts, details about the debtor's assets and creditors, transfers made within a certain period prior to the bankruptcy filing, and other pertinent information. The compliance or Insolvency employee compares the bankruptcy petition and SOFA with financial records obtained in other internal investigations. Details can also be matched against public records. Where inconsistencies are found, there is a potential that the debtor committed fraud. Employees may question the debtor about incongruities at the "341 meeting", also known as the first meeting of creditors. See 11 USC 341. The debtor is required to attend the **341 meeting** and testify under oath and penalties of perjury about their financial affairs and the information provided in the schedules and statements. Any creditor may attend the **341 meeting** and question the debtor. The court can also compel the debtor to appear and be examined under oath and penalties of perjury about any issue in the bankruptcy case at the request of a party in interest, pursuant to Bankruptcy Rule 2004.
- (7) Indications of fraud in bankruptcy cases fit the same pattern as those found in other Collection cases. However, there is the advantage of gathering evidence under oath if the debtor intentionally attempts to defraud the government. The debtor may have:
 - Failed to disclose assets (generally held in a different name) in the SOFA.

- Transferred personal residence, business or other assets for little or no consideration or less than the fair market value within two years of filing bankruptcy.
- A lifestyle that does not match reported financial standing, e.g. lives in a home or drives a vehicle which they don't appear to be able to afford.
- Claimed no bank accounts in their name. Pays expenses using a related third-party bank account, money orders, certified checks or cash.
- Operated or continues to operate more than one business using similar or like names, while failing to file tax returns or pay tax debts on the related entity. The debtor may use the same business equipment while running the related entities. The bankruptcy does not include related businesses.
- Commingled personal income and expenses with Form 1040, Schedule C income and expenses, or with that of another business entity under the debtor's controls.
- Little or no income reported by third-parties (IRP) but reports significant expenses, in particular mortgage interest. In these cases a taxpayer rarely would claim their allowable expenses in hopes of avoiding detection.
- Transferred an asset into a trust while retaining control and possession of the asset. The presence of a trust is frequently a key indicator of fraud, both in and outside of bankruptcy. If the transfer occurred within two years of filing bankruptcy, this transaction can be an indication of fraud.

- (8) Bankruptcy cases are time-sensitive. A Bankruptcy specialist must file a "proof of claim" to record the government's financial interest in the bankruptcy proceeding. When there is an indication of bankruptcy fraud, employees must request a FEA via the *Specialist Referral System (SRS)* at the earliest possible opportunity.

25.1.2.7 (06-09-2015) Employment Tax Fraud

- (1) IRM 1.2.1.5.2, Policy Statement 4-4, pertains to the examination of employment tax liabilities. Frequently, taxpayers fail to appropriately treat as employees, those persons misclassified as "self-employed" or "casual labor." The most common employment tax fraud, however, is not remitting trust fund taxes to the government. The following paragraphs describe the major identified schemes designed to evade reporting and payment of employment tax. Some criminal violations associated with employment tax fraud are Title 26 IRC 7202, Title 26 IRC 7203, Title 26 IRC 7206, Title 26 IRC 7212 and Title 26 IRC 7215. See IRM 4.23.9.6.4, Civil Fraud Procedures. See IRM 25.1.8.3, Employment Tax Violations, which addresses unpaid payroll taxes, under-reported payroll taxes, and delinquent Form 941, Employer's Quarterly Federal Tax Return, for Field Collection investigations. See IRM 4.23.9.6.3, Criminal Fraud Procedures - General, for guidance on assessing the trust fund recovery penalty in cases that may involve criminal proceedings.
- (2) "Pyramiding": A fraudulent practice involving employment taxes occurs where a business collects and withholds taxes from its employees and intentionally fails to remit those funds held in trust to the IRS. Often, a lack of sufficient operating capital leads the business owner to use the trust funds to pay other liabilities, including overhead. The unpaid quarterly employment tax liabilities accumulate or **pyramid**. **Pyramiding** businesses frequently shut down or file for bankruptcy, and then start a new business under a different name. Without sufficient operating capital, the cycle often begins again.

- (3) Employee leasing companies: This industry is a growing area of fraud. An employee leasing company contracts with a client company to handle the client company's administrative duties, often hiring some or all of the client company's employees and leasing back those same employees to the client company. When the leasing company fails to pay the employment taxes, significant tax deficiencies can accumulate in a short span of time because the leasing company's services may be used by several clients. Generally, the employee leasing company, as a service company, does not have significant assets to collect against. When indicia suggest an employee leasing company was established purposefully to evade federal employment taxes or "distance" the client company from employment tax liability, a referral to CI should be considered. Whether the leasing company or the client company, or both, is liable for employment tax underpayment involves technical issues and TEGEDC Area Counsel must be contacted for guidance on how best to pursue the tax deficiencies.
- (4) Cash wages: Payment of cash wages is a common method of avoiding employment tax reporting requirements. Be aware of situations where the taxpayer regularly issues checks to "cash" for large amounts that do not exceed \$10,000. These checks may be used to pay employees off the books and to avoid Currency Transaction Reports (CTRs). See IRM 4.26.5.5.1, Currency Transaction Reports. Employers occasionally pay part of their employees' wages by check on the books and the remainder off the books in cash, especially for overtime or bonus payments. Businesses also pay workers, who should be treated as employees, in cash, as though they were contracted, to avoid paying employment taxes. In these situations, the employers generally do not maintain accurate records of cash wage payments. This scheme is often found in the construction and landscaping industries. The cash wage reporting may be commingled with labor expenses in Cost of Goods Sold or disguised as a deduction for subcontracted labor. The cash wages are generally not reported on employment tax returns, or Form W-2 and Form 1099.
- (5) Fictitious subcontractors: In this scheme, a taxpayer issues checks to shell corporations holding themselves out as legitimate subcontractors. In fact, these entities exist only on paper. They typically do not perform services or have assets. The shell companies are set up by the taxpayer or third parties ("five percenters"). Checks issued to the subcontractors are cashed by local check-cashing services. The check casher charges a fee and the third party, if used, keeps a small percentage of the cash for their services. The remaining cash is returned to the taxpayer and used to pay its workers. Some of the workers may be paid half on the books by check, and half off the books in cash; while other workers, who should be treated as employees but are not, are paid completely off the books. No social security (also known as Federal Insurance Contributions Act) and/or federal income taxes are withheld from these cash payments, and are generally not reported on the taxpayer's employment tax returns, Form W-2 or Form 1099. The shell companies have a propensity for turnover, often to avoid detection.
- (6) CAWR: Combined Annual Wage Reporting is a document matching program that compares the employee wage information reported by the employer to the Internal Revenue Service (IRS) and the Social Security Administration (SSA). An investigation related to the CAWR originates when information from the IRS and SSA does not match. For example, the taxpayer files Form W-2, reporting wages paid to its employees and the withheld employment taxes from those

wages. However, the taxpayer willingly and knowingly does not make deposits of the withheld taxes or file the associated employment tax or information returns for these periods.

25.1.2.8
(11-03-2023)
Excise Tax Fraud

- (1) There are opportunities for fraud in the specialized area of excise tax. In addition to other indications of fraud, the following incidents should be considered to establish taxpayer's knowledge in excise cases:
 - a. Previously filed returns and paid excise tax but stopped filing and paying without explanation.
 - b. Sale of an article at a tax-included price but did not report or pay tax to the government.
 - c. Handling of identical products, considers one taxable and the other not taxable.
 - d. Membership in trade or industry organizations for a number of years.
 - e. Subscriptions to trade publications.
 - f. Answers provided by the taxpayer via a questionnaire or Initial Document Request (IDR).
 - g. Answers to questions when meeting with the taxpayer face-to-face or virtually.

Note: Refer to IRM 4.24.9.7, Excise Tax Fraud - General, for additional information.

- (2) For excise tax purposes, the Trust Fund Recovery Penalty applies only to the communications tax imposed by IRC 4251 and the air transportation taxes imposed by IRC 4261 and IRC 4271. See IRM 20.1.11.4, IRC 6672 Failure to Collect and Pay Over Tax, or Attempt to Evade or Defeat Tax, for additional guidance on how the trust fund recovery penalty may be used in excise tax cases.
- (3) There is an exemption for excise taxes on any article that is exported, see IRC 4221(a)(2). Therefore, this excise tax exemption may lead taxpayers to provide false information and fraudulent documentation which claims the taxpayer exported articles when in fact the article was not exported.

25.1.2.8.1
(11-03-2023)
Excise Tax Fraud—Fuel Taxes

- (1) In most situations, federal claims for refund of motor fuel excise tax may be made by the person who initially filed Form 720, Quarterly Federal Excise Tax Return, to remit tax or by the end user of the fuel.
- (2) In other situations, claims may be filed by a person who neither paid the tax to the government nor used the fuel. These are commonly referred to as **third-party** claims. See IRM 4.24.8.7.4, Third Party Claims.
- (3) The potential for abuse increases because there are multiple, interchangeable forms that can be used to submit claims. For example, Schedule C on Form 720, Form 8849 or Form 4136 attached to an income tax return, can be used to submit a claim for refund. See IRM 4.24.8.3, Claim Form Types. Consequently, there is the potential for multiple claims made on different forms for the same fuel.
- (4) More blatant fraud potential exists when the claimant never actually purchased, sold, used, or blended the fuel. These claims are the most abusive and may be perpetrated by individuals who are not even in the motor fuel business or engaged in any other business.

- (5) Indicators particular to fuel and biodiesel claims:
- a. Credits claimed by suppliers or customers discovered during IDRS research.
 - b. Credits duplicated on income tax or excise tax returns.
 - c. Gross receipts analysis does not reflect market prices.
 - d. Feedstock purchases do not substantiate production.
 - e. No inventory reconciliations/no internal controls.
 - f. No finished product testing by third party.
 - g. Unable to locate suppliers or customers.
 - h. Purchases or sales primarily to related parties.
 - i. Purchases or sales proceeds not reflected in bank accounts.
 - j. Not selling or using biodiesel or renewable diesel as a fuel.
 - k. Minimal physical assets.

25.1.2.8.2
(06-09-2015)
Excise Tax
Fraud—Wagering Tax

- (1) The critical fraud elements prevalent in most illegal wagering cases are:
- The wagering activity must be subject to the wagering tax laws.
 - Failure of the person to register and pay the special tax before accepting the wager and/or failure of the person to file wagering excise tax returns and pay tax.
 - Evidence to prove that the person willfully failed to comply with the law.
- (2) Some examples of critical fraud elements are:
- Destruction of records. The intentional destruction of records is a strong indication of willful intent to avoid the proper computation and payment of excise taxes, and can assist in the development of a criminal fraud referral. When direct evidence is not available, it may be necessary to establish the amounts of taxable wagers and period of operation using indirect evidence.
 - Criminal/Illegal activity. Most federal excise tax wagering cases are illegal enterprises where the individual(s) is arrested and prosecuted by a state law enforcement agency prior to the Excise Office obtaining the case.
 - Cash transactions. Illegal bookmakers for betting deal in strictly cash transactions with no checks or other bank documents used to leave a paper trail.

25.1.2.8.3
(06-09-2015)
Excise Tax
Fraud—Retailer
Schemes

- (1) The fraud issues in retail excise tax normally relate to the retailer. The retailer collects the tax but does not pay it over to the government. The retailer may cover up the collected tax by altering invoices. The retailer may also give false information about to whom the sales were made (a customer exempt from tax) to avoid applying the tax.
- (2) Retail excise tax can also be covered up by using false export claims.

25.1.2.8.4
(06-09-2015)
Excise Tax
Fraud—Heavy Highway
Vehicle Use Tax

- (1) An individual or a company who is required to pay taxes on the Form 2290, Heavy Highway Vehicle Use Tax Return, to obtain state registrations, can falsify documents and understate the number of vehicles to avoid paying the excise tax.
- (2) The requirements for filing the Form 2290 are:

- a. A taxable highway motor vehicle, which includes any self-propelled vehicle designed to carry a load over public highways, whether or not also designed to perform other functions, is registered, or required to be registered, under state, District of Columbia, Canadian, or Mexican law at the time of its first use during the taxable period, and
- b. The vehicle has a taxable gross weight of 55,000 pounds or more.

25.1.2.8.5
(11-03-2023)
Excise Taxes—Willful Failure to Pay

- (1) See IRM 20.1.11.10, IRC 4103 Certain Additional Persons Liable for Tax Where There is Willful Failure to Pay, for guidance on the assertion of the willful failure to pay fuel tax penalty under IRC 4103.

25.1.2.8.6
(11-03-2023)
Section 4103 cases—Referrals to Collection Function

- (1) See IRM 4.24.9.3., IRC 4103 Case Referrals to Collection Function, for guidance on referring potential IRC 4103 cases to the collection function.
- (2) Appropriate notations, such as how the taxpayer designed to avoid reporting and payment of the proper amount of excise tax, must be included in the examination work papers or case file with a copy of the completed referral memorandum. In cases where IRC 4103 does not apply, examiners must annotate the work papers that a referral was considered, but not made, and include the reasons.

25.1.2.9
(04-23-2021)
Return Preparer Fraud

- (1) There are tax return preparers who defraud taxpayers and the United States Treasury by inflating income, deductions, credits, or withholding without the taxpayer's knowledge, with the goal of increasing the overall amount of the taxpayer's refund. The preparer then diverts the refund (or portion thereof) into his or her account or that of a nominee. For example:
 - Some cases may involve the preparer filing the return on paper, where the alterations to the return occur after the taxpayer has approved the return. In other cases; however, the taxpayer has indicated approval of the return by signing Form 8879, IRS e-file Signature Authorization, and then the preparer appears to have altered the return before electronically filing it.
 - In some of the cases, the preparer may split the refund by using Form 8888, Allocation of Refund (Including Savings Bond Purchases), so the taxpayer gets the amount of refund they are expecting, and the preparer asks the IRS to direct deposit the portion of the refund resulting from the inflated items into a bank account under the preparer's control.
 - In other cases, the preparer may have the entire refund direct-deposited into their account, and then wire transfers the amount the taxpayer was expecting into the taxpayer's bank account.
- (2) Taxpayers must provide sufficient documentation to the IRS to support a claim of return preparer fraud.
- (3) Taxpayers must complete Form 14157-A, Tax Return Preparer Fraud or Misconduct Affidavit, to file a claim of preparer fraud or misconduct.

25.1.2.10
(11-03-2023)
FinCEN Query (FCQ)

- (1) FinCEN Query (FCQ) is an on-line database query application. The FCQ application was developed by the Financial Crimes Enforcement Network (FinCEN) as part of the BSA Information Technology Modernization Program and is accessed via the secure FinCEN Portal, <https://bsa.fincen.gov>. The FCQ application supports a wide range of law enforcement and regulatory users for ac-

cess to perform report and data information queries on the millions of BSA reports housed within the FCQ database. The system is designed to provide users with expanded query capabilities, including the ability to query multiple fields, use of four available search options, and use of various search methods to narrow or expand query results.

- (2) FEAs and Emerging Threats Mitigation Team (EMT) members are authorized to request access to FCQ to use as a tool in case development.

25.1.2.10.1
(11-03-2023)

Requesting Access

- (1) OFE personnel requesting access to the FCQ application must certify completion of the required ITM SAR courses prior to requesting access:
 - ITM Briefing 41166, Safeguarding Online Access and Using Suspicious Activity Report (SAR) Info Briefing. This briefing on safeguarding online access and using Suspicious Activity Report (SAR) information is for employees who will have direct electronic access to FCQ.
 - ITM Briefing 36427, Safeguarding, Requesting, and Using Suspicious Activity Report (SAR) Security Briefing. This briefing on SAR security and disclosure procedures is for employees who will use SAR data but who will not have direct electronic access to FCQ.
- (2) Managers of employees requesting access to FCQ must take the required ITM briefing:
 - ITM Briefing 41167, Manager Online Suspicious Activity Report (SAR) Audit Trail Reviews Briefing. This briefing is for managers of employees who will have direct electronic access to FCQ.
- (3) After completing the required training courses, the requesting OFE employee will email the ITM course completion certificates to the OFE program analyst in charge of FinCEN approvals and account creations.
- (4) Once the required training is complete, employees request access to the FCQ system through the Business Entitlement Access Request System (BEARS). The employee will request SYS USER FINCEN QUERY SYSTEM access appropriate for the operating division.

Note: OFE users will request: "SYS USER FINCEN QUERY SYSTEM-IRS SBSE FRAUD PROGRAM FUNCTION (FINCEN QUERY -CURRENCY AND BANKING RETRIEVAL SYSTEM)."

- (5) After approving the BEARS request, the OFE program analyst will create an account on FCQ for the requesting employee. The FinCEN system will generate an automated email to the requesting employee with directions to finalize their account.
- (6) When the OFE employee logs into FCQ for the first time, they must choose the option "Background Check Completed" to finalize their account.

25.1.2.10.2
(11-03-2023)

Search Procedures and Reporting Requirements

- (1) OFE employees with FCQ access are allowed to conduct FCQ searches only when there is a documented business purpose. This purpose can be documented by any of the following:
 - SRS Referral ID number,
 - FITS Control number, or

- EMT Project Number.
- (2) When creating a New Search in FCQ, the user is required to complete the “Agency’s Reference” and “Brief Description” fields.
 - (3) OFE employees must complete the “Agency’s Reference” field as follows:
 - a. When a FEA is doing preliminary research based on an SRS referral, the FEA will input “SRS” and the corresponding SRS referral ID (Example: SRS12345).
 - b. When the research is based on an assigned FITS case, the FEA will input “FITS” and the assigned FITS case number (Example: FITS12345).
 - c. When an EMT project is being researched, the EMT employee or FEA assigned to assist in the project will input month and year of the project and project number (Example: YYMM-Number). If a project number isn’t available, then the EMT employee or FEA will input “Email” and the date of the email (Example: Email MM-DD-YYYY).

Reminder: “Agency’s Reference” cannot include any PII per IRM 10.5.1.2.3.1, Examples and Categories of PII.

- (4) OFE employees must complete the “Brief Description” field as follows:
 - a. For FEAs conducting case research, the **Brief Description** will be “Potential Fraud Development.”
 - b. For FEAs and EMT members working an assigned EMT project, the **Brief Description** will be “Approved EMT Data Analytics Project.”

Note: Additional guidance on FCQ search methods can be found in IRM 4.26.4.5, Researching FinCEN Query.

25.1.2.10.3 (11-03-2023) Annual Audit Procedures

- (1) Every year in August, the OFE program analyst responsible for FinCEN will initiate the annual OFE FinCEN audit. Each FEA and EMT manager will conduct an audit of their employees for September 1- July 31 of the current year by completing the following steps:
 1. The group manager will email a list of their employees with their corresponding email addresses to **SBSE FCQ AUDIT TRAIL* for the date range listed above requesting a FinCEN Query Audit Trail report for each employee. The manager will receive spreadsheets showing each FCQ access made by the employee.
 2. The group manager will review each employee’s audit trail for any discrepancies in “Agency’s Reference” or “Brief Description” as well as making sure each access is an approved SRS referral, FITS case or EMT Project. If there are any discrepancies, the manager and the program analyst will meet with the OFE employee to discuss the issue. If the issue with a particular employee persists into the next year, the manager and program analyst can decide to remove FCQ access for that particular employee.

25.1.2.10.4 (11-03-2023) Program Analyst Procedures

- (1) OFE’s program analyst oversees employee access to FCQ as well as the annual FCQ audit. The analyst will approve or remove BEARS entitlement access as well as create or remove FCQ account access.
- (2) Procedures for FCQ account approvals:

- a. The analyst will make sure they receive the required ITM course certificates as stated above before approving a BEARS entitlement request.
 - b. The analyst will upload the ITM certificates to the Fraud Enforcement Policy SharePoint site.
 - c. Once the BEARS entitlement request is approved, the analyst will then log into FCQ and create the employees' account.
- (3) Annual Audit Procedures:
 - a. Every year in August, an employee from FinCEN will contact the analyst to begin the annual FinCEN audit. FinCEN will send guidance and data relating to the accesses done by OFE employees.
 - b. The analyst will send out a reminder email with the instructions to the FEA and EMT managers regarding the annual audit and what they are required to do.
 - c. The analyst will maintain all records related to FinCEN access and audits on the Fraud Enforcement Policy SharePoint site.
 - d. The analyst will meet with the FinCEN employee and discuss the results of the audit and any issues that arose during it.

25.1.2.10.5
(11-03-2023)
**Maintenance and
Removal of Access**

- (1) FCQ requires biannual training. Each OFE employee with access to FCQ must complete this training to keep their accounts active. The training is located under the "Training/Help" icon on the main FCQ login page. The training is called "Law Enforcement BSA Data Certification Training."
- (2) Employees with FCQ access who leave OFE are required to submit a BEARS request to remove their FCQ access. The program analyst will approve the BEARS request for removal and deactivate the employee's FCQ account.

25.1.2.11
(05-20-2024)
Digital Asset Fraud

- (1) As mentioned in IRM 5.1.18.20, Definition of Digital Assets, digital assets may be a capital asset, inventory, a form of payment to acquire goods or services, compensation, or held as an investment. Since digital assets can be used in many of the same ways as non-digital assets, the general indicators of fraud, located at IRM 25.1.2.3, Indicators of Fraud, can also apply to digital asset cases. While the use of digital assets is not itself an indicator of fraud, there are indicators of fraud that are specific to digital asset cases. Some of these indicators of fraud are listed below.

Note: Digital asset subject matter experts are available to assist IRS personnel with blockchain analysis and/or digital asset tracing to identify many of the indicators of fraud listed below. Points of contact, key terms and concepts, and other resources can be found at the *Digital Assets Knowledge Base*.

25.1.2.11.1
(05-20-2024)
**Indicators of Fraud in
Digital Asset Cases**

- (1)

Examples of Fraud Relating to Unreported Income:
Intentional failure to report a substantial portion of digital asset transactions over multiple years despite knowledge of a reporting requirement.
Reporting of digital asset activity reflected on an information return but intentional failure to report digital asset transactions for which no information return was received/filed.

Examples of Fraud Relating to Unreported Income:

Reporting digital asset activity which occurred at some exchanges but intentional failure to report digital asset transactions which occurred at other exchanges.

Claiming income tax treaty positions for which taxpayers have no connection in order to exempt gains from digital asset transactions.

Solicitation for payment via digital assets in an attempt to evade reporting requirements.

Use of un-hosted wallets to store digital assets in order to avoid reporting requirements.

Intentionally answering “No” to the question of digital asset use on tax returns despite the taxpayer’s knowledge that they:

- Received digital assets as payment for goods or services provided,
- Received digital assets as a reward/award,
- Received new digital assets as a result of mining, staking, or related activities,
- Received digital assets as a result of a hard fork and/or airdrop,
- Disposed of digital assets in exchange for property or services,
- Disposed of digital assets in exchange or trade for another digital asset, or
- Sold a digital asset.

Note: Evidence to support the above activities can be obtained through an interview with the taxpayer and/or return preparer, blockchain analysis, internal research, or review of taxpayer-provided (or summonsed) financial records.

Examples of Fraud Relating to Expenses or Deductions:

Overstatement of digital asset cost basis to reduce gain and/or increase loss.

Overstatement of digital asset valuation to increase charitable deductions.

Participation in activities, such as NFT wash trading/self-dealing, to generate artificial losses.

Fictitious or substantially overstated business expenses related to digital asset mining activity.

Intentional miscategorization of digital asset personal expenditures as business expenses.

Examples of Fraud Relating to Books and Records:

Intentional failure/refusal to provide complete digital asset records/information to a return preparer or compliance employee after repetitive requests.

Submission of altered or false digital asset records to return preparers and/or compliance employees.

Having multiple sets of books for a business which receives digital assets as a form of payment or not maintaining any records to support digital asset activity.

Use of fictitious valuation methods for reporting digital asset income and/or expenses.

Intentional omission of digital asset transactions (in full or part) from the books and records.

Examples of Fraud Relating to Taxpayer Conduct:

Ownership or use of an address with direct receiving exposure from a scam, darknet market, or other high-risk address or entity.

Utilizing digital asset kiosks to convert significant amounts of cash into digital assets or digital assets into cash.

Conversion of physical assets to digital assets in anticipation of, or in response to, IRS actions.

False statements about the location/use of digital assets to return preparers and/or compliance employees.

Association or use of peel chain transactions.

Chain hopping to rapidly convert digital assets from one blockchain to another in order to obscure the source and use of assets.

Examples of Fraud Relating to Methods of Concealment:

Common methods of concealment can be located at IRM 25.1.2.3, Indicators of Fraud. Methods of concealment specific to digital assets, may include:

Direct sending/receiving exposure to mixers/tumblers.

Use of Monero, Dash, Zcash, or other “privacy coins.”

Use of exchanges/services with inadequate or no Know Your Customer (KYC)/Anti-Money Laundering (AML) procedures.

Holding digital asset exchange accounts in the names of nominees where the taxpayer is the beneficial owner.

Use of CoinJoin or other obfuscation techniques/software in order to avoid reporting requirements.

- (2) As stated in IRM 25.1.1.4, Indicators of Fraud vs. Affirmative Acts of Fraud, an indicator of fraud serves as a sign or symptom, or signifies that actions may have been taken for the purpose of deceit, concealment or to make things seem other than what they are. No one indicator of fraud is determinative that fraud is indeed present. However, if you identify any of the above indicators of fraud, complete a *Specialist Referral System (SRS)* request for a consultation with a Fraud Enforcement Advisor.

25.1.2.11.2
(05-20-2024)
IRS Has Repeatedly Informed Taxpayers of the Requirement to Report Digital Asset Transactions

- (1) The IRS has issued multiple notices and information releases to the public to announce digital asset reporting requirements. Some examples of these notices and information releases are listed below:

IRS Has Repeatedly Informed Taxpayers of the Requirement to Report Digital Asset Transactions

In March 2014, the IRS issued Notice 2014-21 and Information Release IR-2014-36, on the income tax treatment of virtual currency, such as bitcoin. The IRS explained that virtual currency is treated as property, rather than currency, for tax purposes. General tax principles that apply to property transactions apply to transactions using virtual currency. This information was supplemented by Notice 2023-34 which was issued in August 2023.

In March 2018, the IRS issued Information Release IR-2018-71 to remind taxpayers to report virtual currency transactions.

In July 2018, the IRS made an announcement of a virtual currency campaign to urge taxpayers to correct their returns as soon as possible if they have not reported virtual currency transactions.

In July 2019, the IRS issued Information Release IR-2019-132 regarding letters to virtual currency owners that potentially failed to report income or did not properly report their transactions advising them to file amended returns and pay back taxes.

In December 2019, the IRS published frequently asked questions (FAQs) to expand upon the examples provided in Notice 2014-21. There have been additions to these FAQs in subsequent years.

In February 2022, the IRS issued Information Release IR-2022-33 expanding a section on the Form 14457, Voluntary Disclosure Practice Preclearance Request and Application, to report virtual currency.

In March 2022, the IRS issued Information Release IR-2022-61 which reminded taxpayers that there is a virtual currency question at the top of the 2021 Form 1040, Form 1040-SR, and Form 1040-NR.

In January 2023, the IRS issued Information Release IR-2023-12 to remind taxpayers that they must again answer a digital asset question and report all digital asset related income when they file their 2022 federal income tax return.

IRS Has Repeatedly Informed Taxpayers of the Requirement to Report Digital Asset Transactions

In January 2024, the IRS issued Information Release IR-2024-18 to remind taxpayers that they must again answer a digital asset question and report all digital asset related income when they file their 2023 federal income tax return. In addition to the digital asset question appearing on Form 1040, U.S. Individual Income Tax Return, Form 1040-SR, U.S. Income Tax Return for Seniors, and Form 1040-NR, U.S. Nonresident Alien Income Tax Return, the digital asset question was also added to Form 1041, U.S. Income Tax Return for Estates and Trusts, Form 1065, U.S. Return of Partnership Income, Form 1120, U.S. Corporation Income Tax Return and Form 1120-S, U.S. Income Tax Return for an S Corporation.

In April 2024, the IRS issued Fact Sheet FS-2024-12 to remind taxpayers that they must answer the digital asset question and report all digital asset related income when they file their 2023 federal income tax return.

- (2) In addition, the IRS has established a *Digital Assets* page at www.irs.gov. IRS personnel should consider these materials and other facts and circumstances of each case to evaluate whether taxpayers can meet the reasonable cause exception for fraud penalties. The facts and circumstances evaluation should include, among other things, an evaluation of: (a) the taxpayer's conduct as discussed herein; (b) the taxpayer's level of sophistication necessary to find these materials; and, (c) the taxpayer's ability to obtain assistance from a knowledgeable professional. See IRM 25.1.1.4, Indicators of Fraud vs. Affirmative Acts of Fraud, for the definition of an indicator of fraud.

25.1.2.11.3
(05-20-2024)

Use of FinCEN in Digital Asset Cases

- (1) One resource that should be utilized in developing a fraud case is research through the Financial Crimes Enforcement Network (FinCEN) Query. Reports generated from this research may indicate that a taxpayer is purchasing physical assets with digital assets and/or conducting suspicious digital asset transactions as identified on Suspicious Activity Reports (SARs). The narrative and/or attachments to these SARs may contain digital asset addresses or transaction hashes which can be used to trace digital asset activity.
- (2) Collection employees can locate FinCEN resources at IRM 5.1.18.14, Financial Crimes Enforcement Network Query (FCQ) System, and IRM 5.1.18.15, Accessing Information on the FinCEN Query (FCQ) System.
- (3) Examination employees can locate FinCEN resources at IRM 4.26.15.4, FinCEN Query System (FCQ) Use in Title 26 Examinations, IRM 4.10.4.7.2, Accessing/Receiving SAR Information in SB/SE, and IRM 4.10.4.7.3, Guidelines for SAR Data Security and Disclosure Considerations.
- (4) The Bank Secrecy Act (BSA) program is a delegee of FinCEN and they provide Servicewide guidance on FinCEN Query (FCQ) at IRM 4.26.4.